BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problems Mailbox.

AA

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-234967
(43)Date of publication of application : 13.09.1996

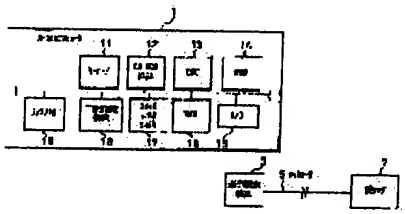
(51)Int.Cl. G06F 9/06
G06F 9/06
G06F 15/00
G09C 1/00
H04L 9/06
H04L 9/14

(21)Application number : 07-037865
(22)Date of filing : 27.02.1995

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : OKUYAMA HIRONOBU
KANAI ATSUSHI
MIYAKE NOBUHISA

(54) DISTRIBUTION METHOD FOR CIPHERED INFORMATION

(57)Abstract:
PURPOSE: To provide a circulation method of ciphered information which can facilitate the separation of responsibility between a program producer and a program receiver by decoding only the uninstalled information when the ciphered information is decoded and without remodeling an installer by separating the inatallation processing from the decoding processing.
CONSTITUTION: All software including an installer are ciphered and stored in a secondary storage 16, and these software are installed in a computer by means of an installation program included in the restored software. Thereby, the decoding processing carried out by the computer of a terminal user is separated from the installation processing. Then the responsibility can be easily separated between a program producer and a person received the ciphered program without remodeling the installer.



LEGAL STATUS

[Date of request for examination] 17.11.1998
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－234967

(43)公開日　平成８年(1996)９月13日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	9/06	４１０		Ｇ０６Ｆ	9/06	４１０Ｂ
		５５０				５５０Ａ
	15/00	３３０	9364－5L		15/00	３３０Ｚ
Ｇ０９Ｃ	1/00		7259－5Ｊ	Ｇ０９Ｃ	1/00	
Ｈ０４Ｌ	9/06			Ｈ０４Ｌ	9/02	Ｚ

審査請求　未請求　請求項の数１　ＯＬ　（全９頁）　最終頁に続く

(21)出願番号　特願平7－37865

(22)出願日　平成７年(1995)２月27日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　奥山　浩伸
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　金井　敦
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(72)発明者　三宅　延久
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

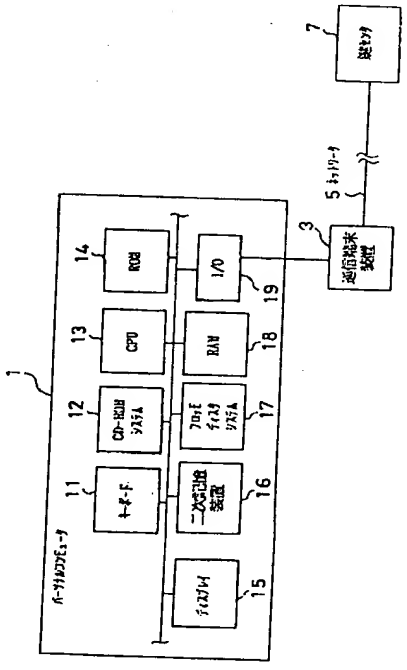
(74)代理人　弁理士　三好　秀和　（外１名）

(54)【発明の名称】　暗号化情報の流通方法

(57)【要約】

【目的】　暗号化された流通情報を復号化する時にインストール前の情報にまでしか復号化せず、インストールは復号化とは独立に行うことによりインストーラの改造を必要とせず、プログラムの制作者と流通者との責任の切り分けを容易にした暗号化情報の流通方法を提供する。

【構成】　インストーラも含めたソフトウェアをすべて暗号化し、復号化されたソフトウェアを二次記憶装置１６に記憶し、復元されたソフトウェアに含まれるインストールプログラムを使用して、コンピュータにソフトウェアをインストールすることにより、端末ユーザのコンピュータでの復号化処理とインストール処理を分離し、インストーラを改造する必要がなく、プログラム制作者と暗号化してプログラムを流通された者との責任の切り分けを容易にすることができる。



1

【特許請求の範囲】

【請求項１】　ネットワークを介してあるいはＣＤ－ＲＯＭを代表とする記録媒体を介して情報流通者により安価にまたは無償で流通している暗号化された流通情報を、該流通情報を復号化する復号化鍵を有する鍵センタからネットワークにより接続された端末に配送した前記復号化鍵を用いて復号化する暗号化情報の流通方法において、

端末のユーザがネットワークを介してまたはＣＤ－ＲＯＭを代表とする記録媒体を介して端末上に入手した前記情報流通者が用意した情報流通用プログラムが購入希望ソフトウェアを端末のユーザに選択させ、そのソフトウェア名を購入リストに記録し、前記購入リストに記録された流通情報がすべて展開できる容量が端末上の二次記憶装置に空いているかどうかをチェックし、空き容量が不十分であれば購入リストをクリアして購入リストを再作成させ、空き容量が十分であれば前記購入リストに記された流通情報を復号化するために必要な復号化鍵を前記鍵センタに要求し、復号化鍵を取得し、前記流通情報を復号化して二次記憶装置に記憶することを特徴とする暗号化情報の流通方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、情報流通機構において特に端末ユーザのソフトウェア流通をより柔軟にし、ソフトウェアの流通性を高める方法に関し、更に詳しくは、ネットワークを介してまたはＣＤ－ＲＯＭ等の記録媒体を介して情報流通者により流通している暗号化された流通情報を鍵センタから配送される復号化鍵を用いて復号化しながらインストールする暗号化情報の流通方法に関する。

【０００２】

【従来の技術】情報を暗号化してネットワークを介してまたはＣＤ－ＲＯＭ等の記録媒体を介して流通させる従来の暗号化情報の流通方法においては、ソフトウェアをインストールする時に予め取得しておいた復号化鍵を用いて、暗号化情報を復号化しながらインストールする方法がとられている。なお、流通情報には、ソフトウェアだけでなく、音楽、動画、辞書等の各種データがあるが、ここでは流通情報を代表してソフトウェアと記述することにする。

【０００３】

【発明が解決しようとする課題】従来、使用されている方法では、復号化処理を組み込むために、ソフトウェア毎に作られている多くのインストーラを改造することが必要である。また、インストール処理と復号化処理が分離されないでインストール処理が完了するため、制作者と暗号化してソフトウェアを流通させた者との責任の切り分けが難しく、混乱の元になるという問題がある。

【０００４】本発明は、上記に鑑みてなされたもので、

2

その目的とするところは、暗号化された流通情報を復号化する時にインストール前の情報にまでしか復号化せず、インストールは復号化とは独立に行うことによりインストーラの改造を必要とせず、プログラムの制作者と流通者との責任の切り分けを容易にした暗号化情報の流通方法を提供することにある。

【０００５】

【課題を解決するための手段】上記目的を達成するため、本発明の暗号化情報の流通方法は、ネットワークを介してあるいはＣＤ－ＲＯＭを代表とする記録媒体を介して情報流通者により安価にまたは無償で流通している暗号化された流通情報を、該流通情報を復号化する復号化鍵を有する鍵センタからネットワークにより接続された端末に配送した前記復号化鍵を用いて復号化する暗号化情報の流通方法において、端末のユーザがネットワークを介してまたはＣＤ－R-OMを代表とする記録媒体を介して端末上に入手した前記情報流通者が用意した情報流通用プログラムが購入希望ソフトウェアを端末のユーザに選択させ、そのソフトウェア名を購入リストに記録し、前記購入リストに記録された流通情報がすべて展開できる容量が端末上の二次記憶装置に空いているかどうかをチェックし、空き容量が不十分であれば購入リストをクリアして購入リストを再作成させ、空き容量が十分であれば前記購入リストに記された流通情報を復号化するために必要な復号化鍵を前記鍵センタに要求し、復号化鍵を取得し、前記流通情報を復号化して二次記憶装置に記憶することを要旨とする。

【０００６】

【作用】本発明の暗号化情報の流通方法では、インストーラも含めたソフトウェア一式をすべて暗号化し、復号化時には復号化されたソフトウェア一式を二次記憶装置に記憶し、端末ユーザがソフトウェア流通方式とは独立にインストールすることを可能としている。

【０００７】更に詳しくは、予め暗号化してあるソフトウェアをネットワークを介してまたはＣＤ－ＲＯＭ等の記録媒体を介して端末ユーザに流通させ、オンラインかまたは人の介在により鍵センタから生成する情報を入手し、端末ユーザのコンピュータでその情報を利用してソフトウェアを復号化し、二次記憶装置に復号化されたソフトウェアを復元し、コンピュータではその復号化鍵を消滅させ、端末のユーザは復元されたソフトウェアに含まれるインストールプログラムを使用して、コンピュータにソフトウェアをインストールすることにより、端末ユーザのコンピュータでの復号化処理とインストール処理を分離している。

【０００８】

【実施例】以下、図面を用いて本発明の実施例を説明する。

【０００９】図１は、本発明の一実施例に係る暗号化情報の流通方法の全体の手順を示すフローチャートであ

3

り、図2は、図1に示す暗号化情報の流通方法を実施するハードウェア構成を示すブロック図であり、図3は、図1に示す暗号化情報の流通方法に使用される端末の構成を示す図である。

【0010】図2に示すように、端末ユーザのパーソナルコンピュータ1は、通信端末装置3からネットワーク5を介して鍵センタ7に接続され、該鍵センタ7から復号化鍵を受信し得るようになっている。パーソナルコンピュータ1は、情報を入力するキーボード11、ソフトウェア等の流通情報が記憶されているCD－ROMを再生するためのCD－ROMシステム12、全体の動作を制御するCPU13、プログラムや固定データ等を記憶するROM14、画像や文字等を表示するディスプレイ15、復号化したソフトウェアを記憶する二次記憶装置16、該二次記憶装置16に記憶されたソフトウェアのバックアップを記録するフロッピーディスクシステム17、各種情報やデータ等を一時的に記憶するRAM18、前記通信端末装置3に接続された入出力インタフェース19から構成されている。

【0011】次に、図1に示すフローチャートおよび図3に示す端末構成を参照して、作用を説明する。

【0012】ソフトウェア提供者は、ソフトウェアを暗号化してネットワークを介してまたはCD－ROM等の記録媒体を介して端末ユーザに流通させる。端末ユーザはネットワークを介してデータベースからまたはCD－ROM等の記録媒体から復号化したい購入ソフトウェアを選択する（ステップS11）。そして、この購入を希望するソフトウェアを購入リストに記録する（ステップS12）。それから、更に購入したいソフトウェアがあるか否かをチェックし、ある場合にはステップS11に戻って同じ動作を繰り返すが、ない場合には、ステップS14に進む。

【0013】ステップS14では、前記二次記憶装置16に復号化後のソフトウェアが展開できる空き容量が十分存在するかどうかをチェックする。なお、復号化鍵は有料である場合も想定しているので、このチェックを行い、復号化結果を保証するものとする。ステップS14のチェックにおいて、二次記憶装置16に空き容量が十分ない場合には、購入リストをクリアして（ステップS15）、最初のステップS11に戻り、再び購入リストを作成するが、二次記憶装置16に空き容量が十分ある場合には、端末ユーザは復号化鍵を配布する鍵センタ7のオペレータと連絡をとるかまたはオンラインで復号化鍵を要求し、復号化鍵を取得する（ステップS16，S17）。なお、この場合、必要ならば、復号化鍵の代金の支払処理も行う。

【0014】復号化鍵を取得すると、この復号化鍵を使用して、目的の暗号化ソフトウェアを復号化し（ステップS18）、この復号化したソフトウェアを二次記憶装置16に記憶する（ステップS19）。それから、端末

4

ユーザはフロッピーディスクシステム17を使用して、二次記憶装置16に記憶されたソフトウェアのバックアップをフロッピーディスクに記録する（ステップS20）。端末ユーザは、取得したソフトウェアを端末にインストールする（ステップS21）。

【0015】課金データベース（DB）の情報に基づいて課金センタ運営者は端末ユーザへ課金処理を行うとともに、使用権販売者に支払処理を行う。

【0016】次に、図4および図5を参照して、流通情報の流通媒体がCD－ROMの場合の処理について説明する。なお、図4および図5は、ステップS16からS17に飛び越し記号Aで連結された一連の処理である。

【0017】図4において、ソフトウェア提供者は、提供しようとするソフトウェアを暗号化する（ステップS31）。この暗号化する対象は通常のパッケージソフトウェアに含まれるプログラム一式である。従って、この時、複数のプログラムファイルやインストールプログラム（コマンド）も暗号化される。

【0018】これらの暗号化されたソフトウェアは編集され、CD－ROMに書き込まれ、端末ユーザに有料または無料で配布される（ステップS32）。端末ユーザはこのCD－ROMを入手し（ステップS33）、該CD－ROMを起動する（ステップS34）。このCD－ROMから購入したいソフトウェアを選択する（ステップS11）。

【0019】以降の処理は、図1で示した処理と同じように、復号化鍵を入手し、CD－ROMに記憶されている暗号化されたソフトウェアを復号化することにより、ソフトウェアを入手し、端末ユーザ自身の手によってフロッピーディスクにバックアップをとり、インストールを行うものであり、同じ処理には同じステップ番号を付し、その詳細な説明を省略する。

【0020】次に、図6および図7を参照して、ネットワークを使用して流通情報を得る場合の処理について説明する。なお、図6および図7は、ステップS16からS17に飛び越し記号Bで連結された一連の処理である。

【0021】図6において、ソフトウェア提供者は、提供しようとするソフトウェアを暗号化する（ステップS41）。この暗号化する対象は通常のパッケージソフトウェアに含まれるプログラム一式である。従って、この時、複数のプログラムファイルやインストールプログラム（コマンド）も暗号化される。

【0022】これらの暗号化されたソフトウェアは、ネットワークを介して読み出し可能なデータベース（DB）に登録される（ステップS42）。それから、端末ユーザはソフトウェア流通方式のための情報流通用プログラムを入手し（ステップS43）、ネットワークを介して購入したいソフトウェアを選択する（ステップS44）。この購入を希望するソフトウェアを購入リストに

5

書き込む（ステップＳ４５）。そして、暗号化された選択ソフトウェアを端末の二次記憶装置１６に記憶する（ステップＳ４６），それから、更に購入したいものがあるか否かをチェックする（ステップＳ１３）。

【００２３】以降の処理は、図１で示した処理と同じように、復号化鍵を入手し、暗号化されたソフトウェアを復号化することにより、ソフトウェアを入手し、端末ユーザ自身の手によってフロッピーディスクにバックアップをとり、インストールを行うものであり、同じ処理には同じステップ番号を付し、その詳細な説明を省略する。

【００２４】なお、上記説明では、悪意のユーザに対する暗号化情報、復号化鍵等の保護については本発明の範囲外であるので、特に説明しないが、別の手段が講じられているものである。

【００２５】

【発明の効果】以上説明したように、本発明によれば、インストーラも含めたソフトウェアをすべて暗号化し、復号化されたソフトウェアを二次記憶装置に記憶し、復元されたソフトウェアに含まれるインストールプログラムを使用して、コンピュータにソフトウェアをインストールすることにより、端末ユーザのコンピュータでの復号化処理とインストール処理を分離しているので、プログラム毎に作成されている多くのインストーラを改造する必要がなく、プログラム制作者と暗号化してプログラムを流通された者との責任の切り分けを容易にすることができる。

6

【図面の簡単な説明】

【図１】本発明の一実施例に係る暗号化情報の流通方法の全体の手順を示すフローチャートである。

【図２】図１に示す暗号化情報の流通方法を実施するハードウェア構成を示すブロック図である。

【図３】図１に示す暗号化情報の流通方法に使用される端末の構成を示す図である。

【図４】流通情報の流通媒体がＣＤ－ＲＯＭの場合の処理を示すフローチャートである。

【図５】流通情報の流通媒体がＣＤ－ＲＯＭの場合の処理を示すフローチャートであり、図４の処理に続く処理を示している。

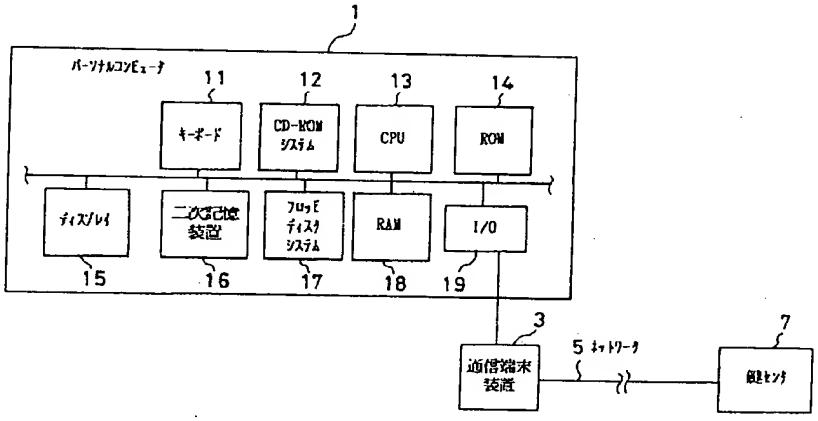
【図６】ネットワークを使用して流通情報を得る場合の処理を示すフローチャートである。

【図７】ネットワークを使用して流通情報を得る場合の処理を示すフローチャートであり、図６の処理に続く処理を示している。

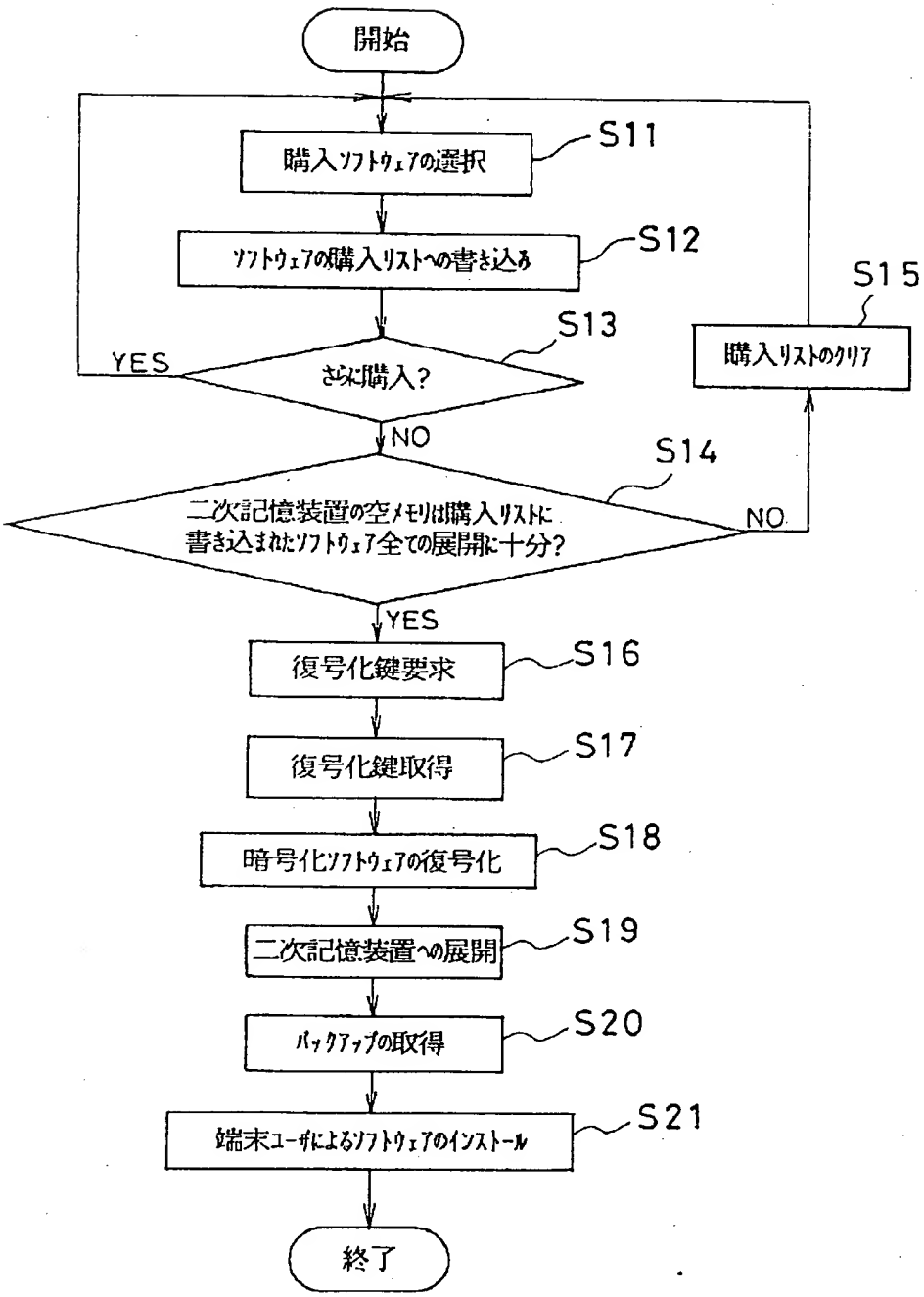
【符号の説明】

１　パーソナルコンピュータ
３　通信端末装置
５　ネットワーク
７　鍵センタ
１２　ＣＤ－ＲＯＭシステム
１３　ＣＰＵ
１６　二次記憶装置

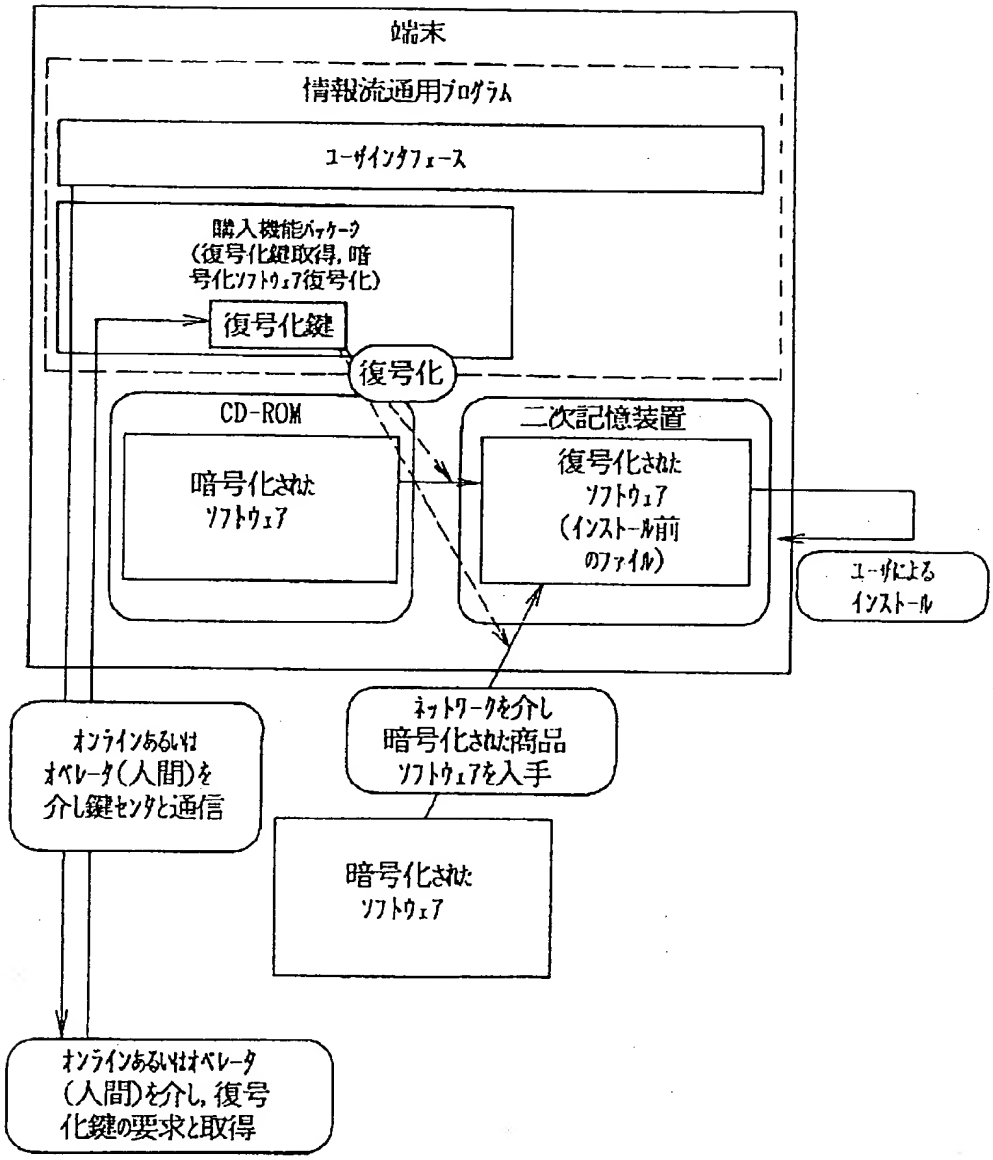
【図２】



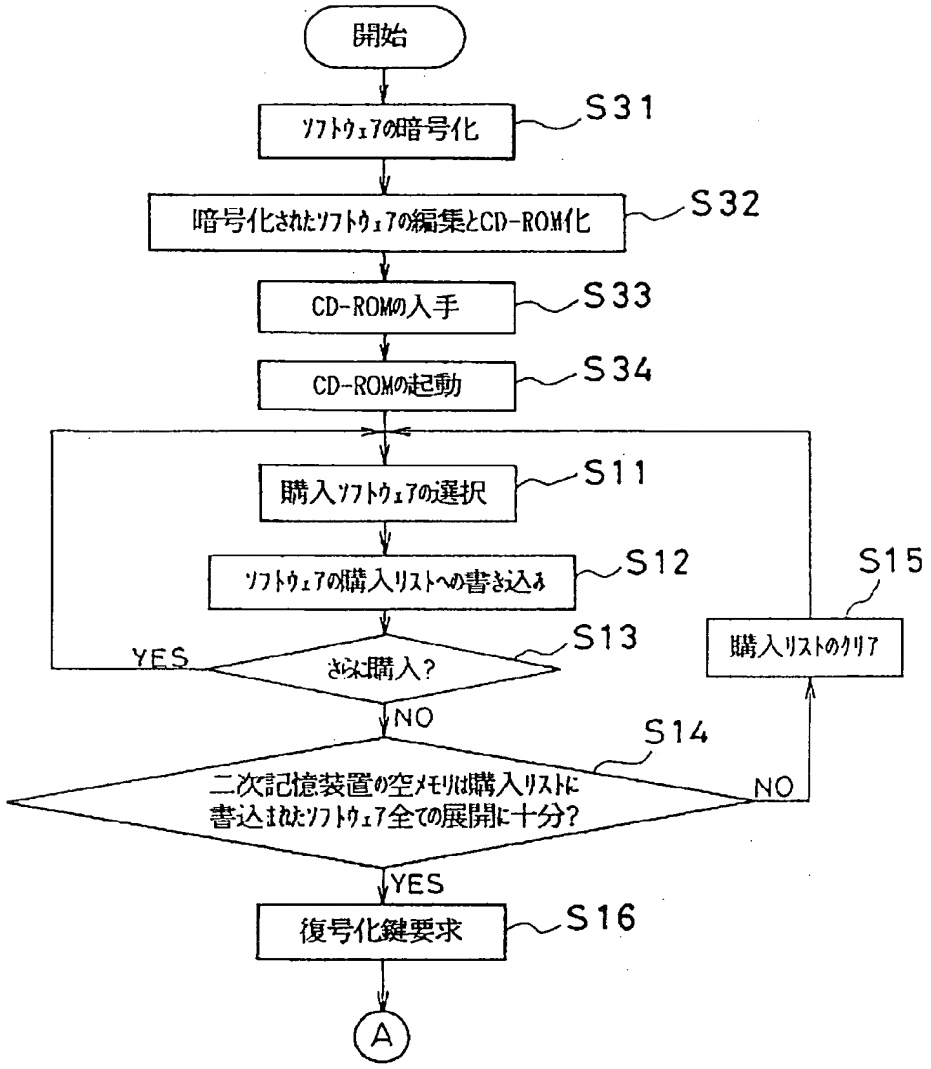
【図１】


開始
購入ソフトウェアの選択
S11
ソフトウェアの購入リストへの書き込み
S12
さらに購入?
S13
YES
NO
購入リストのクリア
S15
二次記憶装置の空メモリは購入リストに書き込まれたソフトウェア全ての展開に十分?
S14
NO
YES
復号化鍵要求
S16
復号化鍵取得
S17
暗号化ソフトウェアの復号化
S18
二次記憶装置への展開
S19
バックアップの取得
S20
端末ユーザによるソフトウェアのインストール
S21
終了

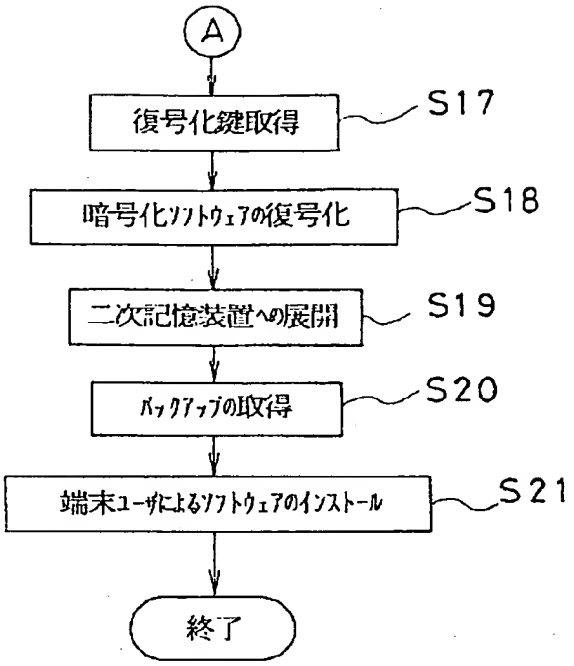
【図３】


端末
情報流通用プログラム
ユーザインタフェース
購入機能パッケージ
(復号化鍵取得，暗号化ソフトウェア復号化)
復号化鍵
復号化
CD-ROM
暗号化された
ソフトウェア
二次記憶装置
復号化された
ソフトウェア
(インストール前
のファイル)
ユーザによる
インストール
ネットワークを介し
暗号化された商品
ソフトウェアを入手
暗号化された
ソフトウェア
オンラインあるいは
オペレータ(人間)を
介し鍵センタと通信
オンラインあるいはオペレータ
(人間)を介し，復号
化鍵の要求と取得

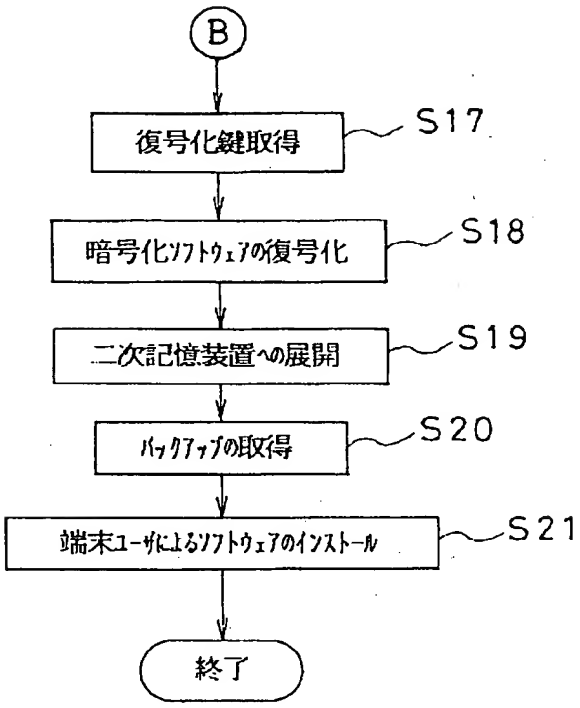
【図４】


開始
ソフトウェアの暗号化
S31
暗号化されたソフトウェアの編集とCD-ROM化
S32
CD-ROMの入手
S33
CD-ROMの起動
S34
購入ソフトウェアの選択
S11
ソフトウェアの購入リストへの書き込み
S12
さらに購入?
S13
YES
NO
購入リストのクリア
S15
二次記憶装置の空メモリは購入リストに書込まれたソフトウェア全ての展開に十分?
S14
NO
YES
復号化鍵要求
S16
A

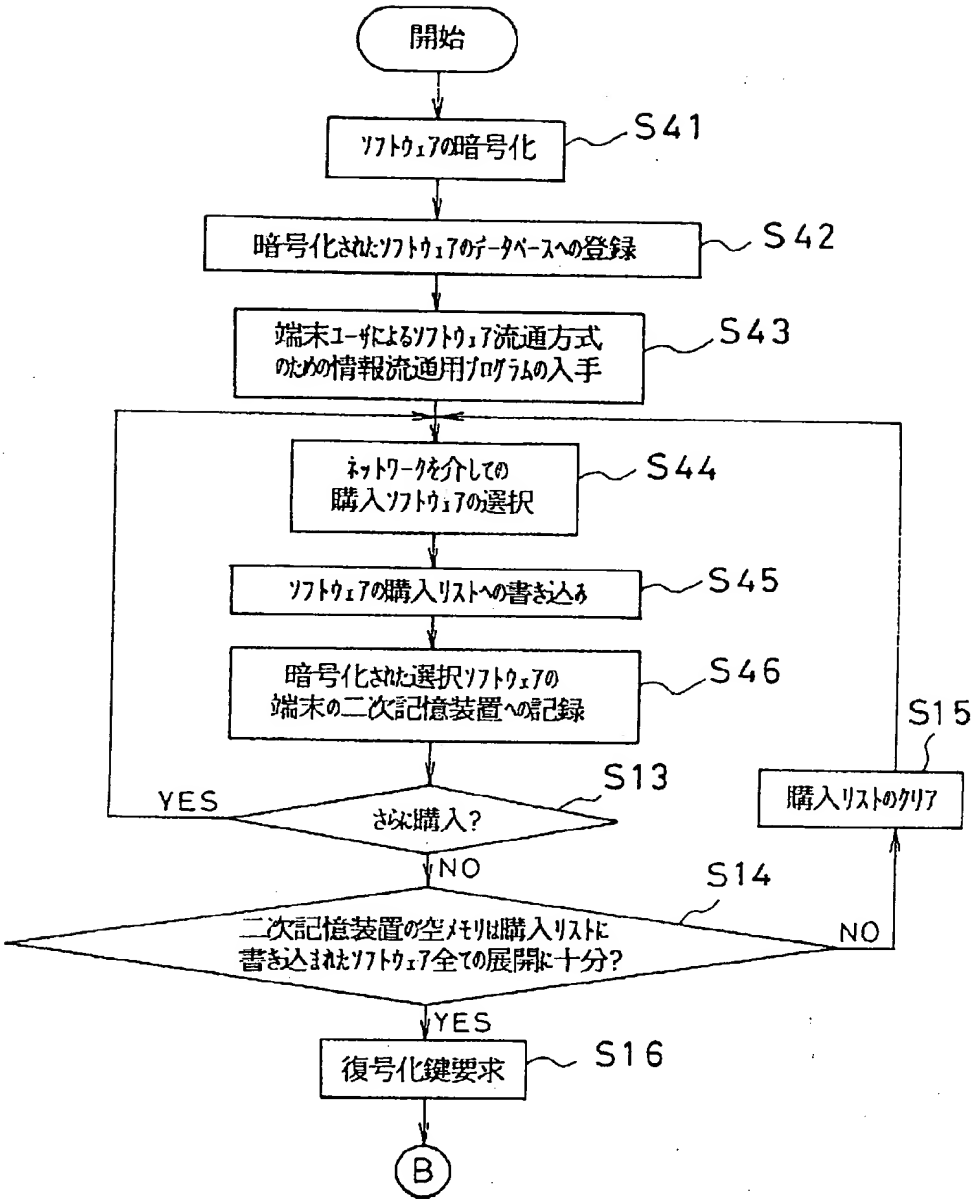
【図５】


A
復号化鍵取得
S17
暗号化ソフトウェアの復号化
S18
二次記憶装置への展開
S19
バックアップの取得
S20
端末ユーザによるソフトウェアのインストール
S21
終了

【図７】


B
復号化鍵取得
S17
暗号化ソフトウェアの復号化
S18
二次記憶装置への展開
S19
バックアップの取得
S20
端末ユーザによるソフトウェアのインストール
S21
終了

【図６】



フロントページの続き

(51) Int. Cl.[6]	識別記号	庁内整理番号	F I	技術表示箇所
H04L 9/14				